UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/654,417	09/04/2003	Philip Kwan	FOUND-0058 (034103-049)	7628

49680 7590 07/29/2008

FOUNDRY-THELEN REID BROWN RAYSMAN & STEINER LLP
P.O. BOX 640640
SAN JOSE, CA 95164-0640

EXAMINER	
ABEDIN, SHANTO	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
07/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/654,417	KWAN ET AL.	
	Examiner	Art Unit	
	SHANTO M Z ABEDIN	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 May 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 September 0203* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *05/05/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the communication filed on 05/05/2008

2. Claims 1- 46 are currently pending in the application.

3. Claims 1-46 are rejected.

4. The examiner notes, upon further examination, new grounds of rejection are found, and presented in this office action.

Double Patenting

5. The examiner notes, a terminal disclosure was filed by the applicant on 03/20/2007 to overcome the previous obvious type double patenting rejection with the co-pending application No. 10/458,628. The terminal disclosure filed on 03/20/2007 had been accepted, and the obvious type double patenting rejections are previously withdrawn.

Response to Arguments

5. The applicant's arguments regarding the previous 35 U.S.C. 103(a) type rejections are fully considered, however, moot in view of new grounds of rejection presented in this office action.

Claim Objections

6. Claims 11 and 12 are objected to because of the following informalities: claims recite the limitations such as "virtual local area network (ULAN)" which seems to have typing error - 'ULAN' should be replaced by 'VLAN'. Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 1-12, 35, 38-39 and 44 are rejected under 35 USC 101 since the claimed invention is directed to non-statutory subject matter.

Regarding claims 1 and 38, they are directed to a layer 2 access device, or an apparatus comprising ports, switching fabric, and control logic, however, according to the specification (Fig 2; Par 0044), these claimed features or components can be optionally implemented in software alone. Therefore, claimed apparatus, or access device lacks any hardware or computer component, and considered to be non-statutory. See MPEP 2106.01.

Regarding claims 2-12, 35, 39 and 44, they are rejected because of their dependencies on claims 1 or 38, and since they further fail to incorporate any computer hardware to the claimed apparatus or device.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-34 and 44-46 are rejected under 35 USC 103 (a) as being unpatentable over Kanuri et al (US 6807,179 B1) in view of Short et al (US 7194554 B1) further in view of Tsuchiya et al (US 7360086 B1)

Regarding claim 1, Kanuri et al teaches a layer 2 network access device for providing network security, comprising:

a plurality of input ports (Fig1, 12.22; Col 3, lines 25-67; multiport switch)

a switching fabric in the layer 2 network access device for routing data received on the plurality of input ports to at least one output port (Fig 1.28; Col 3, lines 25-67; switch fabric; Col 4, lines 7-52; layer 2 switch); and

control logic in the layer 2 network access device (Col 3, line 28 to Col 5, line 65: the switch; MAC module; switching (rules) logic) adapted to authenticate a physical address of a user device coupled to one of the plurality of input ports (Col 3, line 28 to Col 5, line 65; matching MAC addresses).

Kanuri et al fails to teach device adapted to authenticate user information provided by a user of the user device only if the physical address is valid , and to restrict access to the one of the plurality of input ports in accordance with a user policy associated with the user information only if the user information is valid.

However, Short et al discloses network security/ access device adapted to authenticate user information provided by a user of the user device only if the physical address is valid , and to restrict access to the one of the plurality of input ports in accordance with a user policy associated with the user information only if the user information is valid (Fig 2; Col 4, starts at line 12; Col 9, starts at line 8; authenticating, and restricting access based on both user id/ information, and MAC).

Furthermore, Tsuchiya et al discloses network security/ access device adapted to authenticate user information provided by a user of the user device only if the physical address is valid (Col 3,

lines 17-45; Col 10, lines 10-50; Col 14, lines 5-55; authenticating user with the authentication table after matching of the address/ MAC in host table); if authentication of user information indicates the user information is valid, determine whether the user is associated with a VLAN supported by the apparatus (Fig 2, Fig 3; Col 10, lines 10-50; Col 14, lines 5-55); and restrict access to the one of the plurality of input ports in accordance with a user policy associated with the user information; and if the user is not associated with the VLAN, assign the one of the plurality of input ports to a port default VLAN (Col 10, lines 10-50; Col 14, lines 5-55)

Tsuchiya et al , Short et al and Kanuri et al are analogous art because they are from the same field of endeavor of secure network communication. At the time of invention, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Tsuchiya et al and/ or Short et al with Kanuri to design an apparatus wherein network security/ access device utilizes both user provided authentication information, and MAC, and authenticate user information provided by a user of the user device only if the physical address is valid in order to provide a robust and improved communication control mechanism.

Regarding claim 13, it is rejected applying as above as rejecting claim 1, furthermore, Kanuri et al teaches a method for providing network security, comprising:

authenticating in a laver 2 network access device a physical address of a user device coupled to a port of a the network access device (Fig 2:40; associated port, MAC and VLAN information; Col 3, line 28 to Col 5, line 65; matching MAC addresses);

Kanuri et al fails to teach authenticating user information provided by a user of the user device only if the physical address is valid , and to restrict access to the one of the plurality of input

ports in accordance with a user policy associated with the user information only if the user information is valid.

However, Short et al discloses authenticating user information provided by a user of the user device only if the physical address is valid , and to restrict access to the one of the plurality of input ports in accordance with a user policy associated with the user information only if the user information is valid (Fig 2; Col 4, starts at line 12; Col 9, starts at line 8; authenticating, and restricting access based on both user id/ information, and MAC).

Furthermore, Tsuchiya et al discloses network security/ access device authenticating user information provided by a user of the user device only if the physical address is valid (Col 3, lines 17-45; Col 10, lines 10-50; Col 14, lines 5-55; authenticating user with the authentication table after matching of the address/ MAC in host table); if authentication of user information indicates the user information is valid, determine whether the user is associated with a VLAN supported by the apparatus (Fig 2, Fig 3; Col 10, lines 10-50; Col 14, lines 5-55); and restrict access to the one of the plurality of input ports in accordance with a user policy associated with the user information; and if the user is not associated with the VLAN, assign the one of the plurality of input ports to a port default VLAN (Col 10, lines 10-50; Col 14, lines 5-55)

Regarding claim 23, it is rejected applying as above rejecting claim 1, furthermore, Kanuri et al teaches network system, comprising:

a data communications network (Fig 1; Col 3, line 27 to Col 4, line 50; communication between network nodes/ stations/ devices);

a layer2 network access device coupled to the data communications network (Fig 1.28; Col 3, lines 25-67; switch fabric; Col 4, lines 7-52; layer 2 switch); and

a user device coupled to a port of the network access device (Col 3, line 54 to Col 4, line 34; user, or network nodes' attributes/ policies/ information);

wherein the network access device is adapted to authenticate a physical address of the user device (Col 3, line 28 to Col 5, line 65; matching MAC addresses).

Kanuri et al fails to teach device adapted to authenticate user information provided by a user of the user device only if the physical address is valid , and to restrict access to the one of the plurality of input ports in accordance with a user policy associated with the user information only if the user information is valid.

However, Short et al discloses network security/ access device adapted to authenticate user information provided by a user of the user device only if the physical address is valid , and to restrict access to the one of the plurality of input ports in accordance with a user policy associated with the user information only if the user information is valid (Fig 2; Col 4, starts at line 12; Col 9, starts at line 8; authenticating, and restricting access based on both user id/ information, and MAC).

Furthermore, Tsuchiya et al discloses network security/ access device adapted to authenticate user information provided by a user of the user device only if the physical address is valid (Col 3, lines 17-45; Col 10, lines 10-50; Col 14, lines 5-55; authenticating user with the authentication table after matching of the address/ MAC in host table); if authentication of user information indicates the user information is valid, determine whether the user is associated with a VLAN supported by the apparatus (Fig 2, Fig 3; Col 10, lines 10-50; Col 14, lines 5-55); and restrict access to the one of the

plurality of input ports in accordance with a user policy associated with the user information; and if the user is not associated with the VLAN, assign the one of the plurality of input ports to a port default VLAN (Col 10, lines 10-50; Col 14, lines 5-55)

Regarding claim 2, Kanuri et al teaches the network access device of claim 1, wherein the physical address comprises a Media Access Control (MAC) address (Col 5, starts at line 23; MAC address).

Regarding claim 3, Kanuri et al teaches the network access device of claim 1, wherein the control logic is adapted to authenticate the user information in accordance with an IEEE 802. lx protocol (Col 3, starting at line 36: IEEE 802.3).

Regarding claim 4, it is rejected applying as same motivation as applied above rejecting claim 1. Kanuri et al fails to disclose network access device wherein the user policy identifies an access control list. However, Tsuchiya et al discloses network access device wherein the user policy identifies an access control list (Col 2, starts at line 32; control table).

Regarding claim 5, it is rejected applying as above applied rejecting claims 1 and 4, furthermore, Tsuchiya et al discloses the network access device wherein the user policy includes an access control list (Col 2, starts at line 32; sending and receiving information according to the control table).

Regarding claim 6, Kanuri et al teaches the network access device of claim 1, wherein the user policy identifies a Media Access Control (MAC) address filter (Fig 2.40, 2.42; Col 5, starting at line 41; address table including MAC/ VLAN/ Port information; matching MAC addresses) .

Regarding claim 7, Kanuri et al teaches the network access device of claim 1, wherein the user policy includes a Media Access Control (MAC) address filter (Fig 2.40, 2.42; Col 5, starting at line 41; address table including MAC/ VLAN/ Port information; matching MAC addresses).

Regarding claim 8, Kanuri et al fails to teach the network access device of claim 1, wherein the control logic is adapted to send the user information to an authentication server and to receive an accept message from the authentication server if the user information is valid. However, Short et al teaches control logic is adapted to send the user information to an authentication server and to receive an accept message from the authentication server if the user information is valid (Col 3, starts at line 10; AAA / RADIUS server authenticating user id).

Regarding claim 9, Kanuri et al fails to teach the network access device of claim 8, wherein the authentication server comprises a Remote Authentication Dial-In User Service (RADIUS) server. However, Short et al teaches wherein the authentication server comprises a Remote Authentication Dial-In User Service (RADIUS) server (Col 3, starts at line 10; AAA / RADIUS server).

Regarding claim 11, Kanuri et al teaches the network access device of claim 1, wherein the control logic is further adapted to assign the one of the plurality of input ports to a virtual local area network (ULAN) associated with the user information if the user information is valid (Col 5, starting at line 25; matching VLAN information).

Regarding claim 12, Short et al discloses wherein the message comprises a VLAN identifier (ID) associated with the user information, and to assign the one of the plurality of input ports to a ULAN associated with the VLAN ID (Col 3, starts at line 10; VLAN ID)

Regarding claims 44, 45 and 46, they are rejected applying as above rejecting claims 1,13 and 23, furthermore, Short et al discloses user information comprises user name and password (Col 8, starts at line 10). Furthermore, Tsuchiya et al discloses user information comprises user name and password (Fig 3; Col 3, starts at line 20; authentication table/ user information containing username and password).

Regarding claims 10, 18-22, 30-34, they recite the limitations of claims 1, 8-9 and 12, therefore, they are rejected applying as above rejecting claims 1, 8-9 and 12.

Regarding claims 14-15, 17, 24-25, 28-29, they recite the limitations of claims 1-3, 6-7, therefore, they are rejected applying as above rejecting claims 1-3 and 6-7.

Regarding claims 16, 26 and 27, they recite the limitations of claims 4 and 5, therefore, they are rejected applying as above rejecting claims 4 and 5.

9. Claims 35-43 are rejected under 35 USC 103 (a) as being unpatentable over Kanuri et al (US 6807,179 B1) in view of Short et al (US 7194554 B1) further in view of Tsuchiya et (US 7360086 B1) further in view of Volpano (US 7188364 B2).

Regarding claims 38, 40 and 42, Kanuri et al teaches an apparatus/ method/ system for providing network security, comprising:

a data communication network (Col 3, starts at line 26; network packets);

a network access device coupled to the data communication network (Col 3, starts at line 26; switch enabling communication);

a plurality of input ports (Fig1, 12.22; Col 3, lines 25-67; multiport switch);

a switching fabric for routing data received on the plurality of input ports to at least one output port (Fig 1.28; Col 3, lines 25-67; switch fabric; Col 4, lines 7-52; layer 2 switch); and control logic configured/adapted to:

authenticate a physical address of a user device coupled to one of the plurality of input ports (Col 3, line 28 to Col 5, line 65: the switch; MAC module; switching (rules) logic; matching MAC addresses);

wherein the message comprises a VLAN identifier (ID) associated with the user information (Col 5, lines 1-65; determining/ matching VLAN index/ information);

if the user is associated with the VLAN, determine whether the user is associated with a VLAN supported by the apparatus (Col 5, lines 1-20; Col 6, lines 1-40); and assign the one of the plurality of ports to the VLAN associated with the user (Col 5, lines 1-20; Col 6, lines 1-40; switching logic assigning/ selecting ports);

if the user is not associated with the VLAN,

assign the one of the plurality of input ports to a port default VLAN (Col 5, lines 1-20; Col 6, lines 1-40; switching logic assigning/ selecting ports); and

Kanuri et al fails to disclose expressly the device configured/ adapted to authenticate user information provided by a user of the user device only if the physical address is valid; if authentication of user information indicates the user information is valid; and restrict access to the one of the plurality of input ports in accordance with a user policy associated with the user information; and drop packets from the user device if the physical address is invalid; if authentication of the user information indicates the user information is invalid, block all traffic on the one of the plurality of input ports except for packets related to a user authentication protocol; receiving a message from an authentication server, wherein the message comprises a VLAN identifier (ID) associated with the user information; if the user is not associated with the VLAN, block all traffic on the one of the plurality of input ports except for packets related to the user authentication protocol.

However, Short et al discloses network security/ access device configured/ adapted to authenticate user provided authentication information, and MAC (Col 9, starts at line 8); and restrict access to the one of the plurality of input ports in accordance with a user policy associated with the user information (Fig 2; Col 4, starts at line 12; authentication; user id; MAC); and receiving a message from an authentication server, wherein the message comprises a VLAN identifier (ID) associated with the user information (Col 9, starts at line 8; Authentication server authenticating VLAN, MAC and user information).

Furthermore, Tsuchiya et al discloses the device adapted to authenticate user information provided by a user of the user device only if the physical address is valid (Col 3, lines 17-45; Col 10, lines 10-50; authenticating user with the authentication table after matching of the address/ MAC in host table); dropping packets from the user device if the physical address is invalid (Col 3, lines 17-45; Col 10, lines 36-67; Col 14, lines 5-55; discarding/ not sending the packets upon authentication with the host table/ MAC address or port number); if authentication of user information indicates the user information is valid, determine whether the user is associated with a VLAN supported by the apparatus (Fig 2, Fig 3; Col 10, lines 10-50; Col 14, lines 5-55); and restrict access to the one of the plurality of input ports in accordance with a user policy associated with the user information; and if the user is not associated with the VLAN, assign the one of the plurality of input ports to a port default VLAN (Col 10, lines 10-50; Col 14, lines 5-55)

Modified Tsuchiya et al -Short-Kanuri et al system fails to disclose: if authentication of the user information indicates the user information is invalid, block all traffic on the one of the plurality of input ports except for packets related to a user authentication protocol; if the user is not associated with the VLAN, block all traffic on the one of the plurality of input ports except for packets related to the user authentication protocol.

However, Volpano discloses

if authentication of the user information indicates the user information is invalid, block all traffic on the one of the plurality of input ports except for packets related to a user authentication protocol (Col 5, starting at line 30; control frames; EAPOL);

if the user is not associated with the VLAN, block all traffic on the one of the plurality of input ports except for packets related to the user authentication protocol (Col 5, starting at line 30; control frames; EAPOL).

Volpano and Kanuri et al are analogous art because they are from the same field of endeavor of VLAN utilizing bridges/ switches. At the time of invention, it would have been obvious to a person of ordinary skill in the art to combine the teachings of modified Tsuchiya – Short et al- Kanuri et al apparatus/ method/ system with Volpano to design an apparatus further adapted to drop/ filter packets by authenticating utilizing an authentication server, authentication protocol message containing VLAN identifier in order to provide a proper VLAN packet filtering.

Regarding claims 35-37, they recite the limitations of claims 1, 14, 24, 38 and 40, therefore, they are rejected applying as above applied rejecting claims 1,14, 24, 38 and 40.

Regarding claims 39, 41 and 43, Kanuri et al discloses wherein the network access device comprises a layer 2 network access device (Col 3, starts at line 27; the multiport switch enabling communication of layer 2 type data packets; layer 2 switch).

Conclusion

10. **Examiner's note:** Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from

the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

11. **The prior art made of record and not relied upon** is considered closely pertinent to applicant's disclosure:

- **US 2002/0146002 (Sato)** teaches VLAN security device that authenticates both the received MAC and user information; and wherein MAC address is validated/ checked against stored MAC before authenticating the user information. Sato further teaches performing VLAN setting for users to a default port or group based on VLAN and user information.
- **US 6393484 B1 (Massarani)** teaches network security device, or switches for authentication and access control based on MAC address and user information; and wherein MAC addressed is checked/ authenticated prior to user authorization.
- **S. Schmid et al ,** "An Access Control Architecture for Microcellular Wireless IPv6 Networks" discloses an access control mechanism wherein username and password are used to authenticate the user, and MAC address is used to authenticate the user or host node/ device.

12. A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for response will result in ABANDOMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Z Abedin whose telephone number is 571-272-3551. The RightFax number for faxing directly to the examiner is 571-273-3551. The examiner can normally be reached on M-F from 8:00 AM to 5:30 PM. If attempts to reach the examiner by telephone are unsuccessful,

the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Z Abedin

Examiner, AU 2136

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136